Service: Desktop Intrusion Prevention Service

Service Line: LAN and Desktop Services

Status: In production

General Description:
This Desktop Intrusion Prevention Service places a small security agent on each workstation and provides the following protection and features:

- Spyware prevention
- Virtual patching
- Intrusion prevention
- Application protection
- Anti-virus awareness
- Virus prevention
- Memory protection
- Firewall
- Automatic updates

The Desktop Intrusion Prevention Service is a GTA hosted and managed service that uses the security agents placed on the PCs to identify and track security threats and generate alerts to customer designated contacts.

Service Level Targets:
GTA's Desktop Intrusion Prevention Service is based on ISS's Site Protector as a centralized manager of the Proventia Desktop Security Software. The GTA instance of Site Protector will be configured to alert the agency immediately upon identifying agreed upon critical alerts. GTA's implementation of Site Protector will operate on a 24x7 basis with 24 hours advanced notice to all agencies before maintenance outages.

Availability:
Available to state agencies

Limitations:
The product is designed **only** for use with desktops and laptops running a Microsoft operating system, Windows 2000 or newer. The product will not work on Linux or any other operating system.

Prerequisites:
Desktops **must** have access to the Internet or the state's backbone for the security agent to generate alerts.

Pricing / Charges:
The rate for fiscal year 2006 and 2007 and for budgeting for fiscal 2008 is $1.75 per seat per month.

Service Components or Product Features Included in Base Price:

- **Security Agent Configuration Planning** – GTA will consult with customers to help them understand the possible security configurations this service will provide and define the customer's final, desired security agent configuration. GTA will also work with customers to coordinate changes to their security agent configuration.
- **Implementation Planning –** GTA consultants will provide assistance in planning for the implementation of the desktop security agent software on customer desktops. Automated means are preferred, but the software can be deployed via e-mail, web, or CD.
- **Deployment –** The customer will control the deployment of the security agent to customer PCs.
- **Critical Alerts –** Alerts will be generated to a customer-defined list of personnel via e-mail or pager. During configuration planning, customers will be able to determine which alerts they would like to receive.
- **Regular Status Reports** – GTA will provide weekly status reports of desktop security activity. For a list of available reports see the "Other Information" section of this document.

Options Available for an Additional Charge: N/A

Service Components or Product Features Not Included:

- Security alert monitoring
- Server security and monitoring
- Network security and monitoring
- Remediation services - virus, spyware, etc.

What GTA Provides:

- Use of the GTA Command Center to coordinate support
- Upgrades, patches and licenses for centralized components
- Critical alert monitoring, reporting and tracking
- Retention of security data as prescribed by federal and Georgia law, and GTA Policy
- Management of backup and recovery for the central server hosting Site Protector and the group policies.

What the Customer Provides:

- Distribution list for alerts generated by the service

- Responses to the alerts; management of the customer's escalation procedures, notification paths and contact information for incidents
- Designated representative (and alternate) to speak for the customer regarding the initial security agent implementation, and any subsequent changes to the security agent configuration implemented

Service Support:

- GTA provides support to customer IT representatives to resolve service-related issues. Support services should be engaged through the Command Center. The GTA Command Center can be reached at 404-463-3620 or commandcenter@gta.ga.gov.

- The customer provides support for initial user problem analysis and contact personnel for problem resolution support.

Service Issue Escalation:

- **GTA provides** Command Center services for the appointed agency representative to use.

- **The customer provides** a service issue escalation contact list.

Benefits / Advantages:

- Provides valuable insight to the frequency and types of security threats impacting the customer's desktops. As part of the Desktop Intrusion Prevention Service, customers will be provided regular reporting which will provide them with the information required to make the strategic decisions necessary to limit their exposure to desktop security threats.

- Proactively blocks spyware and more than 97% of new and unknown viruses and worms—without an update. The Desktop Intrusion Prevention Service provides advanced virus protection because, rather than relying on signatures for detection, it uses a behavioral system that analyzes the activities of an executable file and detects whole families of malicious code.

- Easy to manage and scales for small to very large deployments. Using a centralized management system, GTA administrators can control 100,000 Desktop Intrusion Prevention Service agents from a single console.

- ISS provides continuous updates to the security protection. These and any configuration modifications are automatically pushed to desktop security agents when they contact the central management console (requires Internet access).

- Provides location-based protection by automatically enabling additional security when a laptop enters a foreign or untrusted network, such as a wireless connection in a coffee shop. This reduces the possibility of these laptops introducing threats to their corporate environments.

- Blocks buffer overflow attacks, which account for a significant portion of all high-risk vulnerabilities. Like a circuit breaker, it automatically trips to protect the system the instant malicious code tries to run.

- Can be used to ensure that users have compliant systems or are running protective software, like the desktop agent or anti-virus, before allowing local access to the corporate network or remote access through a virtual private network (VPN). It can also prevent users from running or even installing banned programs.

- Fits seamlessly within the customer's existing corporate infrastructure and works with Active Directory, most e-mail and Web clients, and popular anti-virus and VPN software.

How to Start this Service:
Customers should contact the GTA Office of Solutions Marketing at gtasolutionsmrktg@gta.ga.gov or 404-651-6964 to be put in touch with their GTA Account Manager.

Related Services and Products: N/A

Other Information: Standard Reports List:

Assessment Reports:

- Operating System Summary: Displays percentage and number of hosts by operating system discovered during an automated network scan.
- Vulnerability Counts: Lists detected vulnerabilities by total number and by percentage.
- Host Assessment Summary: Lists discovered hosts and for each host, identifies network services and vulnerabilities.
- Host Assessment Detail: Detailed list of vulnerabilities and services for each host, including vulnerability remedies and references.
- Operating System Summary by Host: List of hosts scanned and their operating system.
- Service Summary by Host: List of services discovered for each host scanned.
- Vulnerability Counts by Host: Count of vulnerabilities discovered for each host by severity.
- Vulnerability Remedies by Host: List of vulnerabilities and their remedies for each host.
- Vulnerability Names by Host: List of vulnerability names for each host.
- Service Summary: List of services discovered.
- Top Vulnerabilities: Lists the top vulnerabilities by frequency for a specified group and time.

- Vulnerability Summary by Host: List of vulnerabilities and their descriptions for each host.

- Vulnerability Detail by Host: Detailed list of all vulnerability information available for each host.
- Vulnerability by Group: Compares vulnerabilities across subgroups of a selected group.
- Vulnerability by Host: Lists the top hosts by number of vulnerabilities for a specified group and time.
- Vulnerability by OS: Compares vulnerability counts by operating systems.

Attack Activity Reports

- Attacks by Group: Compares attack counts across subgroups of a selected group.
- Top Attacks: Lists the top attack names by frequency for a specified group and time.
- Top Sources of Attacks: Lists the top attack sources by frequency for a specified group and time.
- Top Targets of Attacks: Lists the top attack targets by frequency for a specified group and time.

Audit Reports

- Audit Detail: Provides an audit trail of significant actions performed by SiteProtector users.

Compliance Reports

- Server Protection Report: Displays counts of servers protected and not protected with version details.

Content Filtering Reports

- Top Web Categories: Lists categories with the number of hosts and requests.
- Web Requests: Count of Web requests by category or client.

Desktop Reports

- Desktop Protection Report: Displays counts of hosts protected and not protected with version details.

Management Reports

- Attack Incidents: Lists all attack incidents created for a specified time.
- Attack Status Summary: Displays attack status summary including Security Fusion and blocked events.
- Attack Trend: Attack activity by day/week/month/quarter/year.
- Virus Activity Trend: Virus activity by day/week/month/quarter/year.
- Vulnerability Trend: Vulnerabilities by day/week/month/quarter/year.

Virus Activity Reports

- Top Virus Activity: Lists the top viruses by frequency for a specified group and time.
- Virus Activity by Group: Compares virus activity across subgroups of a selected group.
- Virus Activity by Host: Lists the top hosts by amount of virus activity for a specified group and time.